Title (en)

METHOD FOR OPTIMIZATION OF THE CONNECTION SETUP OF AN SSL PROXY

Title (de)

VERFAHREN ZUR SSL-OPTIMIERUNG FÜR EINEN SSL-PROXY

Title (fr)

PROCÉDÉ D'OPTIMISATION SSL POUR UN MANDATAIRE SSL

Publication

**EP 3425870 A1 20190109 (EN)**

Application

**EP 18181599 A 20180704**

Priority

US 201715643263 A 20170706

Abstract (en)

Described embodiments establish at least one secure connection for a session. An intermediary device may intercept a domain name service (DNS) request from a client. The device may determine, according to the intercepted DNS request and configuration data of the device, that the client is preparing to establish a session with a server. The device may send a client hello message of the device to the server for establishing a first secure connection between the device and the server for the session, prior to the client sending a client hello message of the client for establishing a second secure connection between the client and the device for the session. The second secure connection may be established between the client and the device using a specified value for a session identifier received from the server in response to the client hello message of the device.

IPC 8 full level

**H04L 29/06** (2006.01)

CPC (source: EP US)

**H04L 63/0281** (2013.01 - EP US); **H04L 63/0823** (2013.01 - EP US); **H04L 63/166** (2013.01 - EP US); **H04L 65/1069** (2013.01 - US)

Citation (applicant)

US 9538345 B2 20170103 - SAH SUDISH KUMAR [IN], et al

Citation (search report)

- [XI] US 2016218977 A1 20160728 - LAPIDOUS EUGENE [US], et al
- [A] US 2017093984 A1 20170330 - DHANABALAN PRAVEEN RAJA [IN], et al
- [A] VINCENT BERNAT: "Speeding up SSL: enabling session reuse | Vincent Bernat", 27 September 2011 (2011-09-27), XP055233257, Retrieved from the Internet <URL:http://vincent.bernat.im/en/blog/2011-ssl-session-reuse-rfc5077.html> [retrieved on 20151203]

Cited by

CN113746856A

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

**EP 3425870 A1 20190109**; **EP 3425870 B1 20201209**; US 10567348 B2 20200218; US 2019014088 A1 20190110

DOCDB simple family (application)

**EP 18181599 A 20180704**; US 201715643263 A 20170706